# Security Aspects of Communications in VANETs

Stefan Mihai, Nedzhmi Dokuz, Meer Saqib Ali, Purav Shah, and Ramona Trestian

London Digital Twin Research Centre,
Faculty of Science and Technology,
Middlesex University, London, UK
E-mails: {SM3488, NS1304, MM3440}@live.mdx.ac.uk, {p.shah, r.trestian}@mdx.ac.uk

***Abstract*—The Fourth Industrial Revolution has begun and it promises breakthroughs in Artificial Intelligence, robotics, Machine Learning, Internet of Things, Digital Twin, and many other technologies that tackle advancements in the industries. The trend is headed towards automation and connectivity. In the automotive industry, advancements have been made towards integrating autonomous driving vehicles into Intelligent Transport Systems (ITS) with the use of Vehicular Ad-Hoc Networks (VANETs). The purpose of this type of network is to enable efficient communication between vehicles (V2V communication) or vehicles and infrastructure (V2I communication), to improve driving safety, to avoid traffic congestion, and to better coordinate transport networks. This direction towards limited (or lack of) human intervention implies vulnerability to cyber attacks. In this context, this paper provides a comprehensive classification of related state-of-the-art approaches following three key directions: 1) privacy, 2) authentication and 3) message integrity within VANETs. Discussions, challenges and open issues faced by the current and next generation of vehicular networks are also provided.**

***Index Terms*—Keywords: VANET, authentication, privacy, message integrity**

## I. Introduction

The latest developments in both automotive and communications industries, especially related to the emerging 5G networks, Internet of Vehicles and adoption of Vehicle-to-Everything (V2X) connectivity, are fuelling significant transformations in terms of driving quality of experience (QoE). The future 5G-V2X paradigm aims at enabling effective connected cars communication as well as fully automated driving that could increase road safety and improve traffic management. However, in order to enable support for these services as well as a new set of related applications (e.g., traffic p rediction, i ntelligent n avigation s ystems, cooperative collision avoidance systems, etc.) one of the key requirements is the provisioning and security of ultra-reliable low latency communication (URLLC) which cannot be guaranteed by the current underlying networks. The highly dynamic nature of the vehicular networks along with the heterogeneity of wireless infrastructures for connected cars (e.g., IEEE 802.11p, LTE-A, etc.) as well as the variety of vehicular applications (e.g., safety, traffic management, infotainment, etc.) makes the resource management, security and the low latency communication requirements a significant c hallenge t hat c annot be handled by traditional networking solutions.

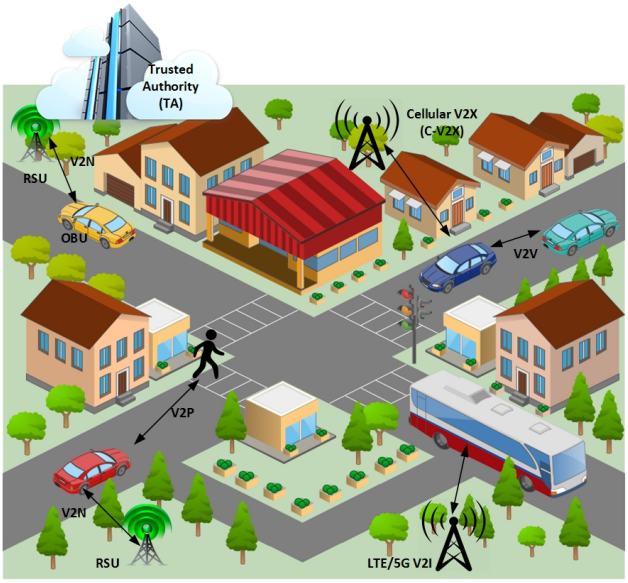


Fig. 1. Heterogeneous Vehicular Networks Environment

As illustrated in Fig. 1, a Heterogeneous Vehicular Networks (HetVNets) environment, consists of the coexistence of different wireless technologies like cellular Base Stations (BS) (e.g., LTE/5G), Road Side Units (RSUs) and On-Board Units (OBUs) based on cellular vehicle to everything (C-V2X) as well as Dedicated Short-Range Communications (DSRC), respectively. The aim of this HetVNets environment is to provide Vehicle to Infrastructure (V2I), Vehicle to Network (V2N), Vehicle to Pedestrian (V2P) and Vehicle to Vehicle (V2V) connectivity to overcome the sporadic connectivity issues of highly mobile and dynamic environments. Because of the widely deployment of the LTE network, it makes it a promising solution to enable V2N communication. Another option is the use of DSRC systems which are designed to provide robust, low-latency, and high-throughput services for V2I and V2V communications making them suitable for safety and non-safety applications. However, because of their sparse deployment and short range they provide intermittent connectivity. Thus, the coexistence of these technologies creates a HetVNets environment able to provide a continuous vehicular connectivity and enables the support for connected and automated vehicles (CAVs). Thus, the advancements in the development of CAVs led to the need of a commu-

nication medium between them, to allow coordination and prevention of incidents. In this sense, Vehicular Ad Hoc Networks (VANETs) have emerged, which are spontaneous networks that allow the exchange of information between traffic participants, providing a foundation for building new vehicular applications that go beyond the scope of accidents prevention.

The many services offered by VANETs heavily rely on Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. A vehicle can broadcast messages, to other vehicles or to the infrastructure, about the weather, traffic reports, anomalies in the road system, accidents, etc. These messages can affect environmental awareness, traffic mobility, and emergency services responsiveness, so it is important that they are accurate, correct and trustworthy. In order to address these challenges many different solutions have been proposed in the research literature. However, despite the amount of research done in this area, there is no global solution that will completely respect the three security requirements identified in [1], such as:

- Privacy and traceability: only a Trusted Authority (TA) (see Fig. 1) should be able to correctly reveal the identity of a message's sender, while keeping it hidden from other third-party listeners;
- Authentication: the messages have to be signed by the senders so that only legitimate traffic participants receive authorization to join the network;
- Message integrity: the messages have to arrive to their destination unaltered.

In this context, this paper presents a comprehensive survey on the latest approaches related to the three key security requirements, such as Privacy, Authentication and Integrity within the context of vehicular networks. The rest of the paper is structured as follows: Section II delves into the latest proposals for privacy-preserving mechanisms. Section III evaluates authentication mechanisms that have surfaced over the last few years, Section IV explores the way message integrity can be assured, while discussions on the challenges and open issues related to the three directions surveyed are provided in Section V. Lastly, Section VI draws the conclusions.

## II. Privacy

In order for the V2V technology to be effective in supporting V2V safety applications, the vehicles must periodically broadcast Basic Safety Messages (BSM) conveying critical vehicle state information to their neighbours or infrastructure and prevent potential collisions. In this context, one of the vital requirements for public acceptance of VANET deployment is privacy. The anonymity of the exchanged information in the network should be kept and the messages should be protected in the presence of an unapproved observer and any information about its sender should not be revealed. Moreover, the actions of the sender should not be linked to its source.

As seen in previous studies, data gathered from basic safety messages can contain GPS location information and this can lead to profiling and uniquely identifying the person using this particular vehicle [2].

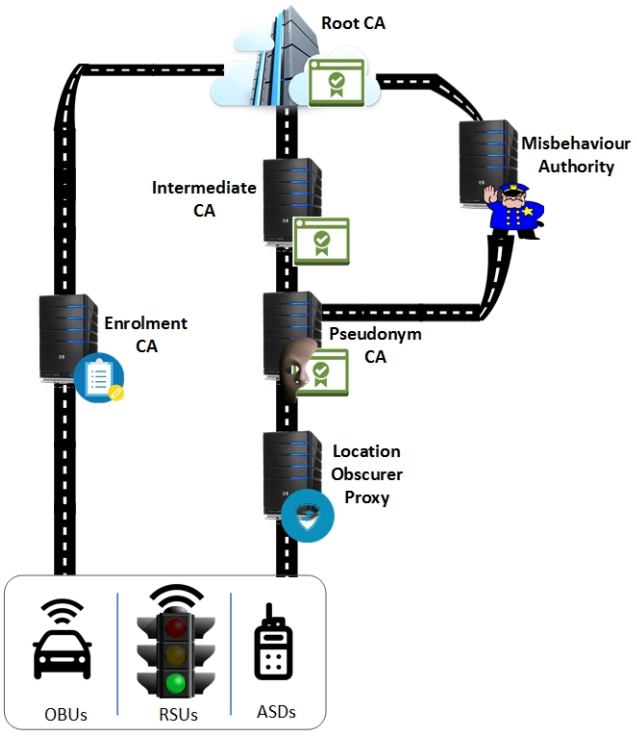


Fig. 2. Security Credential Management System Architecture

The Crash Avoidance Metrics Partners LLC together with the U.S Department of Transportation have developed a Security Credential Management System (SCMS) for V2X communication to overcome the deep privacy concerns of the public. The system requires the connected vehicles to enroll into the SCMS and obtain security certificates from certificate authorities (CAs). The certificates are then attached to the messages exchanged as part of a digital signature to build trust among participants, similar to the public-key infrastructure concept. A simplified architecture of SCMS is presented in Fig. 2 [3] and consists of: V2V or V2I enabled device (e.g., On-Board Units, Road-Side Units, After-market Safety Device, etc.); Enrolment CA will issue enrolment certificates to the connected devices; Location Obscurer Proxy will hide the location of the requesting device and prevents the mapping of the network address to location; Pseudonym CA will issue short-term certificates to the connected devices; Misbehaviour Authority will process misbehaviour reports and identifies potential misbehaviour by devices; the Root CA will provide the system wide trust through certificates issues to all entities involved; and the Intermediate CA will shield the root CA from traffic and attacks. Certificate Revocation Lists (CRL) [4] are used to distribute the revocation information in case a certificate owner is involved in malicious behaviour. However, because the pseudonyms are changed frequently to guarantee security and privacy, this increases the revocation efficiency. A malicious user is revoked by adding all its pseudonyms to the CRL making the updating and distribution procedure of

the CRL list result in large message overheads. This makes the SCMS to be expensive [3] as it will have to deal with large certificate revocation lists while considering the storage limitations on the connected devices.

To overcome these drawbacks, several extensions to the SCMS have been proposed in the literature [5], [6], [7]. Michelson et al. [5] investigate a new way for reporting interference to DSRC networks and propose to clone a second instance of the subsystem used to report untrustworthy digital certificates within SCMS and use it to deliver reports of possible interference events to a Spectrum Misbehavior Authority. The authors make use of a real experimental setup to demonstrate the viability of the interference detection schemes within IEEE 802.11p devices. Jha et al. [6] extend the SCMS with cross certification capabilities. Considering the scenario where several autonomous regions may have their own trust roots, the authors propose a cross-certified trust root where vehicles from one region may validate BSM messages of vehicles from another region that has been cross-certified between the two trust roots. The performance evaluation validated the proposed algorithm under an equal mixture of local and cross-certified vehicular traffic. Bao et al. [7] propose a distributed framework for providing efficient certificate revocation service by making use of the blockchain concept. The proposed solution significantly reduces the size of the Certificate Revocation List as well as the communication overhead and shortens the processing time.

Despite the amount of research done in this area, the pervasive nature of current and future autonomous and connected vehicles makes the privacy issues one of the key challenges. This is because, the nature of the vehicular networks, requires some user privacy data to be open to trusted third-parties (e.g., police, accident rescue, etc.) in case of emergency situation (e.g., accidents) while also enabling the detection and tracking of malicious behaviour within the network. Consequently, the following privacy issues are of concern for the next 5G V2X architecture [8]: (1) identity privacy - deals with the disclosure of identity information that could be linked to a specific user and expose the subscriber's identity. (2) content privacy - deals with the disclosure of sensitive information from different types of content that could result in user privacy breaches. (3) contextual privacy - deals with the disclosure of services a specific user is accessing by linking the source and destination of a packet within the communication path. (4) location privacy - deals with the disclosure of the current and past locations of a specific user.

## III. Authentication

Another key challenge when dealing with security issues in vehicular communications, is the authentication. Authentication is done by signing the outbound messages with the sender's identity in a way that respects the aforementioned principles. In this way, the receivers can confirm the messages' validity. To accomplish this, a number of protocols have been proposed, using different communication patterns: (1) V2I authentication, in which the identity of a vehicle is verified by the fixed RSU; (2) group-based authentication, in which vehicles are authenticated by a Group Leader, who is in turn authenticated by the RSU; or (3) V2V authentication, where the identity of a vehicle is confirmed through an exchange of locality information between vehicles.

### A. V2I authentication

DSRC enables V2V and V2I communication by building wireless ad-hoc networks in a given area. DSRC messages contain safety and traffic information and they are broadcast through 100ms long time slots [9]. This means that, in a VANET, each vehicle would transmit 10 messages per second to its neighbouring vehicles and RSU, and each of them would have to be signed. One of the most widely used authentication mechanism is the digital signature used by the public key infrastructure (PKI) technology. PKI is an asymmetric cryptosystem using two keys: a public one and a private one. However, given the significant message overhead this technique induces, it can only be used in a V2I setting, where the authentication procedure is more centralised: instead of having the vehicles authenticate each other, the closest RSU will verify the messages.

To reduce processing time and requirements, Zhang et al. [10] proposed an Identity-based Batch Verification (IBV) protocol which relieves PKI's need for certificates and relies instead on fake identities and private keys generated by each vehicle's tamper-proof device (TPD) (assumed to be invulnerable to any kind of security risks). The premise of this solution is assigning a unique identifier to each vehicle's TPD, henceforth called a real identity, which will ensure traceability by the TA. The TPD will create an array of random pseudo-identities and private keys from the real identity using a random variable, the ElGamal encryption algorithm, and identity-based cryptography. Every 100ms, a vehicle will send out a tuple containing one pseudo-identity chosen from the list, the useful message, and a digital signature computed with the help of the corresponding private keys. Since the vehicle has a list of fake identities at its disposal and each message will be using a different digital signature, this paper claims that there is no linkability between the messages, eliminating the threat of man-in-the-middle (MITM) attacks. While linkability is indeed made difficult by this protocol, it is not impossible, since each vehicle only has a finite list of pseudo-identities and private keys that it signs its messages with.

Other issues with this authentication scheme are exposed in [1]. The authors point out how each pseudo-identity is strictly connected to the real identity, and every 100ms, the vehicle broadcasts its fake identity along with the message and digital signature, thus exposing the vehicle to impersonation attacks. In fact, the broadcast messages offer enough information for any third-party listener to also successfully reveal the real identity of the vehicle, compromising its privacy. [1] proposes introducing another parameter, a *shared secret* between the RSU and the vehicle, to contribute to the generation of the digital signature, thus eliminating the one-to-one connection between the pseudo-identity and generated signature. The

shared secret is generated by the TA and communicated only once using the PKI.

Both of these approaches use the infrastructure to authenticate the messages. However, in a dense traffic scenario, the RSU could be overloaded with messages that it has to authenticate one by one. The IBV protocol puts forward a batch authentication scheme whose duration depends on the number of applied operations, rather than the size of the batch. However, this approach is prone to significant data loss because if one signature is not valid, the RSU will drop the whole batch. [1] comes up with a verification scheme that focuses on finding invalid signatures into the batch by applying a binary search algorithm. First, the whole batch is checked. If an error is found, instead of dropping the batch, it will be split in half and the batch verification will be applied again on the valid half. The process stops when an inconsequential batch size is achieved. This approach is more efficient at preventing data loss, but at the same time it is more time consuming because of its repetitive structure.

### B. Hybrid authentication

To provide context for this hybrid authentication approach, we are going to revisit the initial issue of the generally accepted approach for an authentication scheme - the digital signature using PKI. As mentioned before, the overhead induced by this technique is so large that, in a congestion scenario, the RSU would not be able to process the high volume of messages in the 100ms window provided by DSRC. In order to relieve some of the RSU's load, one solution would be group-based authentication techniques, in which the RSU or the CA would need only to assign group digital signatures to a conglomeration of vehicles, rather than to each car in part.

Hasrouny et al. [11] propose such a scheme, making use of a hierarchical structure inside the group. The authors introduce the notion of a Group Leader (GL) - the vehicle responsible with the key generation and distribution within the 300m-radius group of at least two vehicles. The GL is the first vehicle in a given area that authenticates with the RSU. Each other vehicle will broadcast a tuple containing its identity, location, a timestamp and status. The leading entity's responsibility is to listen for new nearby vehicles' messages and authenticate them into the group by communicating the group ID and newly generated encryption keys. It is noteworthy that these two parameters will be modified each time a member joins or leaves the group, providing protection against eavesdropping and privacy violation. However, this proposed scheme needs additional security measurements to ensure true protection, since, as the authors admit, it does not account for the fact that the trustworthiness of the group depends on the trustworthiness of its leader. Also, this approach assumes that all traffic participants respect the speed limitations, or at least they do not surpass them by a lot. This means that a high speed vehicle passing by low-speed groups will force the Group Leaders to generate new encryption keys once the vehicle enters their 300m radius and again when it leaves it, inducing additional processing time. Instead, that one vehicle could be its own *group*, independent of the others, because of its significantly higher speed.

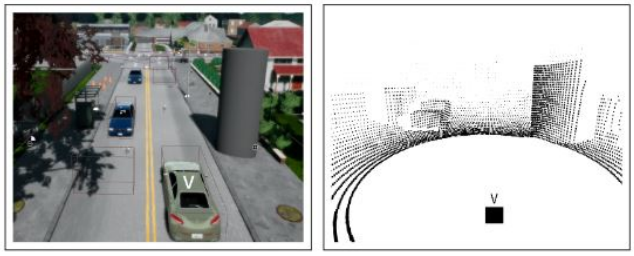

Fig. 3. Lidar capture from a real environment [12]

### C. V2V authentication

The third approach to vehicle authentication in VANETs is the V2V authentication scheme, in which no trusted authorities are involved in verifying the identities of the traffic participants. Lim et al. [12] propose an innovative approach, using LIDAR systems in combination with camera sensors to securely authenticate the messages transmitted in a VANET. The authors explain how, since vehicles communicate through the DSRC technology and traffic messages are transmitted every 100ms, small overheads and quick authentication mechanisms have to be implemented. Before reception, the messages have to be verified and the sender has to be authenticated by the receiving vehicle.

To achieve this, cameras and Lidars are used to scan the environment as illustrated in Fig. 3 and generate localization maps containing the current position, as well as the distance and angles to surrounding objects. Then, vehicles communicate their maps and compare them. If the relative positions of the vehicles to each other matches, then the messages are authenticated. This will prevent man-in-the-middle attacks. However, they do not provide a traceability mechanism, so a malicious vehicle can still send out disorienting information in a traffic scenario and no trusted authority would be able to relate the driver's identity to the incidents.

Table 1 provides an overview of the methods used for ensuring secure authentication. It can be noted that the IBV scheme and the BS scheme have the least damaging disadvantages in terms of security. Taking into account the efficiency of the signature-verification schemes they put forward, the BS scheme solves its predecessor's packet loss problem, although it induces a load-proportional delay.

## IV. Message Integrity

Data integrity assists in defining accuracy, consistency and completeness of the message content used during the communication process. Data integrity is a process of sending information or data from various sources through which users can receive it in a secured manner without any manipulations or alterations to the original data. For VANETs, data integrity can be improved through the use of PKI, cryptography revocation mechanisms, as well as trust management techniques that will avoid the nodes trying to drop, modify, or inject new messages into the communication path [13].

TABLE I
SUMMARY OF AUTHENTICATION METHODS

| | Advantages | Disadvantages |
|---|---|---|
| *IBV scheme (V2I)* | • Fast algorithm<br>• Lower transmission overhead than PKI | • Batch dropped for one invalid signature<br>• Limited sets of pseudo-identities |
| *BS scheme (V2I)* | • Even faster algorithm<br>• Lower rates of packet loss | • Trades encryption efficiency for smaller delay<br>• Binary-search induces delay |
| *Group-based scheme (Hybrid)* | • Significantly reduce RSU workload | • Security depends on credibility of GL<br>• Frequent key generation increases GL workload |
| *LIDAR scheme (V2V)* | • Does not rely on infrastructure<br>• Robust against MITM attacks | • No non-repudiation guarantee<br>• Large processing workloads |

Using the traditional digital signatures within messages to ensure privacy and integrity of the communication, becomes challenging in VANET due to the very large number of public/private key pairs that need to be stored by the vehicles. Additionally, as these keys must be updated/changed often it puts even more pressure on the security of key distribution, management and storage. To overcome these challenges, Guo et al. [14] propose the use of a group signature-based security scheme that achieves authenticity, data integrity, anonymity, and accountability. The proposed scheme will allow group members to sign messages on behalf of the group without revealing the identity of the group member who signed.

Lin et al. [15] introduced a social-tier-assisted packet forwarding protocol, referred to as STAP, that enables the receiver-location privacy preservation in VANETs. The authors define the social tier as a virtual tier formed by social spots, such as shopping malls, busy streets, etc. The RSUs are then deployed at these main social spots to form the STAP and achieve data integrity.

Another group signature and identity-based signature (GSIS) was introduced in [16]. The authors make use of the group signature to secure the communication between OBUs and OBUs. Whereas, a signature scheme using ID-based cryptography (IBC) is implemented in the RSUs to digitally sign the messages and ensure its authenticity. The proposed solution can also be used to trace each vehicle in case of misbehaviour.

A dynamic data integrity auditing scheme is proposed in [17] to support data privacy protection in VANETs. A system model of the data integrity auditing is illustrated in Fig. 4 and consists of three main entities: *Tenant* - who is in fact the data owner and represents the variety of sensing devices within the vehicle that needs to outsource the data collected to the cloud service provider. *Cloud Service Provider* - provides the computing, storage and network resources required by the tenant. *Third-Party Auditor* - is performing the professional data integrity auditing for an authorized tenant by challenging the cloud service provider. It also shares a group of decryption

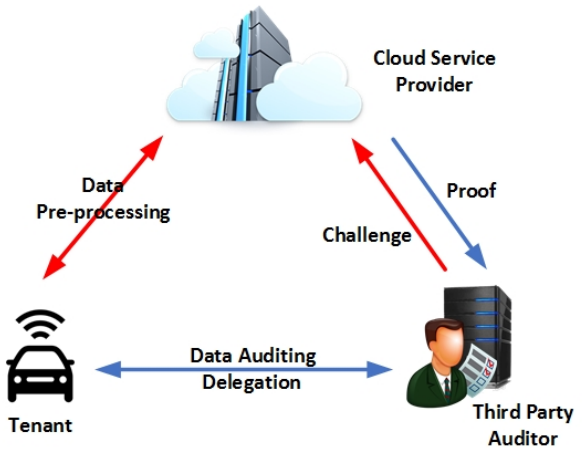


Fig. 4. System model of the data integrity auditing [17]

keys with the tenant. Additionally, bilinear pairing mapping and Boneh-Lynn-Shacham digital signature mechanism were used to ensure that the third-party auditor cannot steal data privacy during the process of data integrity auditing.

Trying to overcome the security risks that appear when the vehicles nodes send their sensor data to a trusted center, Zhang et al. [18] proposed a data security sharing and storage system based on the consortium blockchain (DSSCB).The authors propose the use of bilinear pairing for elliptic curves to ensure the reliability and integrity when transmitting the data to a node. Additionally, the consortium blockchain technology together with the use of smart contracts provides a decentralized, secure and reliable database maintained by the entire network.

## V. REMAINING CHALLENGES AND OPEN ISSUES

The future 5G-V2X paradigm aims at enabling effective connected cars communication as well as fully automated driving that could increase road safety and improve traffic management. However, in order to enable support for these services and a new set of related applications (e.g., traffic prediction, bird's eye view at the road intersection, intelligent navigation systems, 4K live video streaming, cooperative collision avoidance systems) one of the key requirements is provisioning of ultra-reliable low latency communication which cannot be guaranteed by the current underlying networks. Apart from the communication challenges, any misbehavior or malicious alternation within this highly dynamic environment where there is a significant number of messages exchanged among entities could lead to catastrophic accidents. Consequently, the communication security including the message authentication and data integrity are of paramount importance for attack prevention [19] within the future cooperative connected intelligent transportation environment.

Some of the most common attacks on data integrity and authentication within VANETs that need to be overcome are identified as follows [20]: *Masquerading Attack* - where the attacker makes use of a registered user ID and password to enter the system and broadcast false messages; *Replay Attack* - where the attacker aims at repeating or delaying transmission

fraudulently; *Message Tampering Attack* - where the attacker modifies or alters messages for transmission [21]; *Illusion Attack* - where malicious data from sensors is collected and used to generate traffic warning messages that may create illusions to cars at its neighborhood [22]. This illusion attack could cause car accidents, traffic jams and could decrease the VANETs performance.

Apart from the traditional attacks, such as eavesdropping, man in the middle attack, or impersonation, some more advanced attacks could be used to capture private information within the VANETs, such as [8]: *packet analysis attack* - where the sender identity is disclosed by analyzing a packet; *packet tracing attacks* - where the source and destination of a packet could be traced; *linkage attacks* - the pseudonyms of a user are linked based on the public information; *movement tracking attacks* - where the vehicle is traced based on its physical position and moving patterns from captured messages; *identity revealing attacks* - where the identity, moving path, and physical position of a specific vehicle are predicted from routine traffic messages; *collusion attacks* - information about a target user could be disclosed by collaborative adversaries; *inference attacks* - where a target user is identified based on the differences between multiple subjects; and *deanonymization/reidentification attacks* - the target user is re-identified by analyzing the correlations and differences of a large volume of data.

It is obvious that there are many remaining open issues that need to be addressed, and that the safety implications of the future transportation system cannot be taken lightly as the cyber security and the preservation of privacy and information about the drivers, pedestrians and the road infrastructure is of paramount importance to avoid catastrophic scenarios.

## VI. Conclusions

The advancements in technology lead the way towards a connected intelligent cooperative transportation system. This paper discusses the most important aspects of security in VANETs and provides a comprehensive survey of existing proposed techniques for ensuring privacy, authentication, and message integrity within the context of vehicular networks. However, the mainstream uptake depends on closing the gap for the remaining open issues in terms of secure communication between vehicles as well as the road infrastructure. From the challenges identified in this work, it is clear that a standardised approach is required and the governance will need to ensure flexibility and resiliency while maintaining the necessary levels of security and privacy.

## References


[1] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Security and privacy issues for inter-vehicle communications in vanets," in *2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops*, June 2009, pp. 1–3.

[2] M. Kamrani, R. Arvin, and A. J. Khattak, "Extracting useful information from basic safety message data: An empirical study of driving volatility measures and crash frequency at intersections," *Transportation Research Record*, vol. 2672, no. 38, pp. 290–301, 2018. [Online]. Available: https://doi.org/10.1177/0361198118773869

[3] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, Dec 2018.

[4] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for vanet," in *Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking*, ser. VANET '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 88–89. [Online]. Available: https://doi.org/10.1145/1410043.1410063

[5] D. G. Michelson, H. Noori, and Q. Ramsay, "Interference detection and reporting in ieee 802.11p connected vehicle networks," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, Sep. 2019, pp. 1–6.

[6] S. Jha, C. Yavvari, and D. Wijesekera, "Pseudonym certificate validations under heavy vehicular traffic loads," in *2018 IEEE Vehicular Networking Conference (VNC)*, Dec 2018, pp. 1–7.

[7] S. Bao, A. Lei, H. Cruickshank, Z. Sun, P. Asuquo, and W. Hathal, "A pseudonym certificate management scheme based on blockchain for internet of vehicles," in *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, Aug 2019, pp. 28–35.

[8] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5g vehicle-to-everything services: Gearing up for security and privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, Feb 2020.

[9] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, July 2011.

[10] C. Zhang, R. Lu, X. Lin, P. . Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, April 2008, pp. 246–250.

[11] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Group-based authentication in v2v communications," in *2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, April 2015, pp. 173–177.

[12] K. Lim and K. M. Tuladhar, "Lidar: Lidar information based dynamic v2v authentication for roadside infrastructure-less vehicular networks," in *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2019, pp. 1–6.

[13] C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[14] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *2007 Mobile Networking for Vehicular Environments*, 2007, pp. 103–108.

[15] X. Lin, R. Lu, X. Liang, and X. Shen, "Stap: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets," in *2011 Proceedings IEEE INFOCOM*, 2011, pp. 2147–2155.

[16] X. Lin, X. Sun, P. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[17] B. Shao, G. Bian, Y. Wang, S. Su, and C. Guo, "Dynamic data integrity auditing method supporting privacy protection in vehicular cloud environment," *IEEE Access*, vol. 6, pp. 43 785–43 797, 2018.

[18] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58 241–58 254, 2019.

[19] Y. J. Abueh and H. Liu, "Message authentication in driverless cars," in *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, 2016, pp. 1–6.

[20] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)," *Sensors*, vol. 19, no. 16, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/16/3589

[21] R. Mishra, A. Singh, and R. Kumar, "Vanet security: Issues, challenges and solutions," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 1050–1055.

[22] N. Lo and H. Tsai, "Illusion attack on vanet applications - a message plausibility problem," in *2007 IEEE Globecom Workshops*, 2007, pp. 1–8.